Deutscher Bundestag **Drucksache 18/9117**

18. Wahlperiode 04.07.2016

Kleine Anfrage

der Abgeordneten Andrej Hunko, Annette Groth, Niema Movassat, Dr. Alexander S. Neu und der Fraktion DIE LINKE.

Uploadfilter bei Kriminalämtern und Internetunternehmen für sogenannte extremistische oder radikalisierende Inhalte

Das internationale „Counter Extremism Project" (CEP) hat eine Software vorgestellt, mit der extremistische Inhalte beim Upload entdeckt werden sollen (Pressemitteilung Counter Extremism Project vom 17. Juni 2016). Das Verfahren basiert auf PhotoDNA, einer Anwendung die von Microsoft ursprünglich für die Bekämpfung von Kinderpornografie entwickelt wurde. Möglich ist die Detektion von Video- und Audioinhalten. Die Erkennungsquote liegt angeblich bei 98 Prozent. PhotoDNA funktioniert nach dem sogenannten Robust Hashing und erstellt einen digitalen Fingerabdruck der Datei. Der Abgleich erfolgt mit einer Hash-Datenbank, die entweder bei den Unternehmen oder auch Behörden geführt wird. Außer Microsoft haben bereits mehrere Internetdienstleister, darunter Facebook, Google, Youtube und Twitter, PhotoDNA auf ihren Servern installiert. Die Firmen scannen dabei auch Inhalte, die von den Nutzerinnen und Nutzern in der privaten Cloud gespeichert werden. Werden dort kinderpornografische Inhalte entdeckt, können die zuständigen Strafverfolgungsbehörden eine Meldung erhalten. Die Fälle werden dann auch international verfolgt, mindestens einmal hat das Bundeskriminalamt (BKA) einen solchen Hinweis von US-Behörden erhalten (golem.de vom 13. Januar 2015). Das BKA hat im Jahr 2012 selbst die Software PhotoDNA zu „Testzwecken" beschafft (Bundestagsdrucksache 17/11299).

Vergangenen Sommer hatte die Europäische Union eine „Meldestelle für Internetinhalte" bei der Polizeiagentur Europol eingerichtet. Strafverfolgungsbehörden und Geheimdienste aus den Mitgliedstaaten der Europäischen Union können dort Inhalte zur Entfernung melden, Europol reicht diese dann an die Internetunternehmen weiter. Die privaten Internetdienstleister haben selbst keinen Zugriff auf die Polizeidaten. Deshalb hat die Europäische Kommission im Dezember 2015 ein „Forum der Internetdienstleister" gestartet, um die Firmen selbst zur Kontrolle des Internets anzuhalten (www.cilip.de vom 19. November 2015). Das „Forum" soll „Instrumente" zur Bekämpfung terroristischer Propaganda im Internet und in den sozialen Medien entwickeln. Ziel ist die Einrichtung einer öffentlich-privaten Datenbank mit bereits gefundenen bzw. entfernten Inhalten. Laut einer Mitteilung der Europäischen Kommission (COM(2016) 230 final vom 20. April 2016) arbeiten die Unternehmen „unter voller Einbeziehung von Europol" an der gemeinsamen Meldeplattform. Dabei kommt vermutlich ebenfalls die von Microsoft entwickelte Software PhotoDNA zur Anwendung. Das Bundesministerium des Innern bestätigt, „die technische Identifizierung gleicher bzw. ähnlicher Internetinhalte" erfolge anhand von Hashwerten (Bundestagsdrucksache 18/8845). Ein solcher Uploadfilter sei aus Sicht der Bundesregierung „bei den Unternehmen anzusiedeln". Fraglich ist jedoch, wo die benötigte Datenbank mit

Hashwerten von Dateien mit „extremistischen oder terroristischen Inhalten“ geführt wird. Ebenfalls unklar ist, ob dort lediglich solche Internetinhalte gespeichert werden, die bereits einmal hochgeladen wurden, oder ob europäische Kriminalämter (inklusive Europol) dort auch unveröffentlichtes Material zur etwaigen Löschung hinterlegen können.

Im Hinblick auf die sitzungsfreie Zeit des Deutschen Bundestages und die Qualitätssicherung der Antworten erklären sich die Fragesteller mit einer Fristverlängerung für die Bearbeitung der Kleinen Anfrage einverstanden.

Wir fragen die Bundesregierung:

1. Welchen Inhalt hat nach Kenntnis der Bundesregierung ein „Verhaltenskodex“, den die Europäische Kommission am 31. Mai 2016 vorgestellt hat und der mit den Diensteanbietern Facebook, Twitter, YouTube und Microsoft abgestimmt wurde (Bundestagsdrucksache 18/8845)?
2. Wann und wo soll dieser „Verhaltenskodex“ nach Kenntnis der Bundesregierung veröffentlicht werden?
3. Welche weiteren Beteiligten haben den „Verhaltenskodex“ nach Kenntnis der Bundesregierung unterzeichnet, bzw. was ist hierzu geplant?
4. Auf welche Weise wollen die Unternehmen nach Kenntnis der Bundesregierung „stärker gegen illegale Hassbotschaften auf ihren Plattformen vorgehen“?
5. Auf welche Weise haben welche Bundesbehörden in der Vergangenheit mit dem „Counter Extremism Project” kooperiert oder von dort Analysen erhalten?
6. Was ist der Bundesregierung über Pläne des „Counter Extremism Project” (CEP) bekannt, die Internetanbieter zur Einführung einer Software zu bewegen, mit der extremistische Inhalte beim Upload entdeckt werden sollen?
7. Welche Internetanbieter haben einen solchen Filter nach Kenntnis der Bundesregierung bereits eingeführt?
8. Welche technischen Werkzeuge zur automatisierten Erkennung von extremistischen Inhalten hält das Bundesinnenministerium derzeit für prinzipiell geeignet?
9. Auf welche Weise hat das BKA die zu „Testzwecken“ beschaffte Software PhotoDNA eingesetzt?
   a) Auf welche Bild- und Videodatenbanken wurde dabei zugegriffen?
   b) Seit wann ist PhotoDNA nach den Tests beim BKA nicht mehr im Einsatz?
10. Inwiefern wird PhotoDNA nach Kenntnis der Bundesregierung auch bei der Polizeiagentur Europol eingesetzt oder getestet bzw. was ist hierzu geplant?
11. Auf welche Gesichtsbilder kann das BKA außer den in INPOL (das beim BKA betriebene elektronische Informationssystem der Polizei) eingestellten, biometrischen Fotos für einen computergestützten Lichtbildvergleich im Einzel- oder im Regelfall zugreifen?
12. Was ist der Bundesregierung darüber bekannt, welche Inhalte bzw. Formate mit der Software PhotoDNA erkannt werden können?
13. Wie hoch schätzt sie die Erkennungsquote der Anwendung?

14. Was ist der Bundesregierung darüber bekannt, auf welche Datenbanken die von einigen Providern bereits eingeführte Software PhotoDNA für den Abgleich zugreift?
15. In welchen bzw. wie vielen Fällen haben Bundesbehörden Meldungen ausländischer Strafverfolgungsbehörden erhalten, wonach PhotoDNA Inhalte auch in der privaten Cloud von Beschuldigten aufgespürt hat und erst dies schließlich zu Ermittlungen deutscher Kriminalämter führte?
16. Von welchen konkreten Behörden stammten die Hinweise?
17. Was ist der Bundesregierung darüber bekannt, in welchen EU-Mitgliedstaaten Meldestellen für extremistisches, terroristisches oder „radikalisierendes“ Material im Internet eingeführt wurden oder werden, und wo sind diese angesiedelt?
18. Was ist der Bundesregierung über technische Aspekte der gemeinsamen Meldeplattform von Europol und den Internetunternehmen bekannt?
19. Inwiefern soll dort zur „Identifizierung gleicher bzw. ähnlicher Internetinhalte“ die Software PhotoDNA zur Anwendung kommen?
20. Welche Haltung vertritt die Bundesregierung zur Frage, ob die gemeinsame Meldestelle Uploads lediglich auf Inhalte überprüft, die bereits einmal hochgeladen wurden, oder ob europäische Kriminalämter (inklusive Europol) dort auch unveröffentlichtes Material zur etwaigen Löschung durch die Internetanbieter hinterlegen können?
21. Was ist der Bundesregierung darüber bekannt, auf welche Weise das britische Projekt „Research, Information and Communications Unit“ (RICU), das dem dortigen Innenministerium untersteht, an EU-Vorhaben zur Entwicklung von „Gegenpropaganda“ beteiligt ist (http://cage.ngo/publication/we-are-completely-independent/)?
    a) Welche Gruppen der „Zivilgesellschaft“ werden von EU-Projekten, an denen die RICU beteiligt ist, gefördert oder unterstützt?
    b) Auf welche Weise haben dem Bundesinnenministerium nachgeordnete Behörden bislang mit der RICU zusammengearbeitet?
22. Welchen Inhalt hatte die EMPACT-Maßnahme „Cybercrime – cyber attacks“, die das BKA gemeinsam mit dem spanischen Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), der französischen Gendarmerie Nationale, der niederländischen Polizei und dem kroatischen Innenministerium durchführte (www.europol.europa.eu/sites/default/files/publications/empact_01_oap.2015_grants_awarded_0.pdf)?
23. Welche automatisierte Verfahren zur Auswertung von sozialen Medien bzw. deren Integration in Fall- oder Vorgangsbearbeitungssysteme kommen bei den dem Bundesinnenministerium nachgeordneten Behörden zum Einsatz (heise.de vom 28. Juni 2016)?
24. Welche Marktsichtungen oder Studien hat das Bundesinnenministerium hierzu durchgeführt oder beauftragt?

25. Was ist der Bundesregierung über die Funktionsweise der Software rsNetMAn der Firma rola Security Solutions/ T-Systems bekannt?
    a) Wie viele Webseiten oder Einträge in sozialen Medien werden laut dem Hersteller für die Analyse in rsNetMAn ausgewertet?
    b) Welche weiteren Recherchefunktionen können über rsNetMAn ausgeführt werden (etwa Wildcardsuche, fragmentarische Suche, phonetische Suche, Ähnlichkeitssuche, Komplexrecherche, geobezogene Recherche)?
    c) Mit welchen Einschränkungen ist über die Software rsNetMAn auch die Suche nach visuellen Inhalten möglich?
    d) Inwiefern wird für den Einsatz von rsNetMAn schon jetzt nach extremistischen, terroristischen oder „radikalisierenden" visuellen Inhalten gesucht?

Berlin, den 4. Juli 2016

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333